9/14/00

A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new non-provisional applications under 37 CFR 1.53(b)

Attorney Docket No. 004860.P2436 Total Pages 2

First Named Inventor or Application Identifier "J" Leslie Vogell III

Express Mail Label No. EL627466614US

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, D. C. 20231

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

1. X Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. X Specification (Total Pages 36)
(preferred arrangement set forth below)
- Descriptive Title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claims
- Abstract of the Disclosure

3. X Drawings(s) (35 USC 113) (Total Sheets 6)

4. X Oath or Declaration (Total Pages 5)
   a. X Newly Executed (Original or Copy)
   b. ___ Copy from a Prior Application (37 CFR 1.63(d))
   (for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**
   i. ___ DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. ___ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ___ Microfiche Computer Program (Appendix)

7. ___ Nucleotide and/or Amino Acid Sequence Submission

(if applicable, all necessary)

a. ____ Computer Readable Copy
b. ____ Paper Copy (identical to computer copy)
c. ____ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. X Assignment Papers (cover sheet & documents(s))
9. ____ a. 37 CFR 3.73(b) Statement (where there is an assignee)
   X b. Power of Attorney
10. ____ English Translation Document (if applicable)
11. ____ a. Information Disclosure Statement (IDS)/PTO-1449
    ____ b. Copies of IDS Citations
12. ____ Preliminary Amendment
13. X Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. ____ a. Small Entity Statement(s)
    ____ b. Statement filed in prior application, Status still proper and desired
15. ____ Certified Copy of Priority Document(s) (if foreign priority is claimed)

16. Other: Certificate of Express Mail with copy of postcard showing contents of Express Mail package.

17. **If a CONTINUING APPLICATION,** check appropriate box and supply the requisite information:

___ Continuation ____ Divisional ____ Continuation-in-part (CIP)

of prior application No: _____

18. **Correspondence Address**

____ Customer Number or Bar Code Label _____
(Insert Customer No. or Attach Bar Code Label here)

or

X Correspondence Address Below

NAME Sheryl Sue Holloway, Reg. No. 37,850

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

ADDRESS 12400 Wilshire Boulevard

Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (408) 720-8598 FAX (408) 720-9397

PTO/SB/17(6/99)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL FOR FY 2000

TOTAL AMOUNT OF PAYMENT ($) $1492.00

Complete if Known:
Application No. Not Yet Assigned
Filing Date Filed Herewith
First Named Inventor "J" Leslie Vogel III
Group Art Unit Not Yet Assigned
Examiner Name Not Yet Assigned
Attorney Docket No. 004860.P2436

METHOD OF PAYMENT (check one)

1. [X] **The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:**

Deposit Account Number 02-2666
Deposit Account Name

[X] **Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17**

---

2. X **Payment Enclosed:**
X **Check**
____ **Money Order**
____ **Other**

FEE CALCULATION

1. **BASIC FILING FEE**

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	690	201	345	Utility application filing fee	690.00
106	310	206	155	Design application filing fee	
107	480	207	240	Plant filing fee	
108	690	208	345	Reissue filing fee	
114	150	214	75	Provisional application filing fee	

SUBTOTAL (1) $ 690.00

2. **EXTRA CLAIM FEES**

		Extra Claims		Fee from below		Fee Paid
Total Claims	45	– 20** =	25	X 18	=	450.00
Independent Claims	7	– 3** =	4	X 78	=	312.00
Multiple Dependent					=	

**Or number previously paid, if greater; For Reissues, see below.

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	78	202	39	Independent claims in excess of 3
104	260	204	130	Multiple dependent claim, if not paid
109	78	209	39	**Reissue independent claims over original patent
110	18	210	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) $ 762.00

Patent fees are subject to annual revisions. Small Entity payments must be supported by a small entity statement, otherwise large entity fees must be paid.
See Forms PTO/SB/09-12

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for response within first month	
116	380	216	190	Extension for response within second month	
117	870	217	435	Extension for response within third month	
118	1,360	218	680	Extension for response within fourth month	
128	1,850	228	925	Extension for response within fifth month	
119	300	219	150	Notice of Appeal	
120	300	220	150	Filing a brief in support of an appeal	
121	260	221	130	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive unavoidably abandoned application	
141	1,210	241	605	Petition to revive unintentionally abandoned application	
142	1,210	242	605	Utility issue fee (or reissue)	
143	430	243	215	Design issue fee	
144	580	244	290	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	40.00
146	690	246	345	For filing a submission after final rejection (see 37 CFR 1.129(a))	
149	690	249	345	For each additional invention to be examined (see 37 CFR 1.129(a))	

Other fee (specify) _____

Other fee (specify) _____

SUBTOTAL (3) $ 40.00

*Reduced by Basic Filing Fee Paid

SUBMITTED BY:

Typed or Printed Name: Sheryl Sue Holloway

Signature _____ Date September 12, 2000

Reg. Number 37,850 Deposit Account User ID 02-2666 (complete if applicable)

004860.P2436 PATENT

UNITED STATES PATENT APPLICATION

for

USER CONTROL OF A SECURE WIRELESS COMPUTER NETWORK

Applicant:

"J" Leslie Vogel III

prepared by:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 Wilshire Boulevard
Los Angeles, CA 90026-1026
(408) 720-8598

USER CONTROL OF A SECURE WIRELESS COMPUTER NETWORK

FIELD OF THE INVENTION

This invention relates generally to wireless computer networks, and more particularly to establishing a secure wireless network.

COPYRIGHT NOTICE/PERMISSION

BACKGROUND OF THE INVENTION

As the number and type of resources available to a networked computer increases, the need to connect a computer into a network regardless of the location of the computer also increases. Because of the physical limitations inherent in wired networks, wireless network connections are growing in popularity. With the increase in the use of wireless networks comes the requirement to protect the data being exchanges since wireless signals are more easily captured than signals transmitted over a physical connection.

One approach to the problem of wireless connection security is addressed by the IEEE in the 802.11 standard for *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Draft International Standard ISO/IEC 8802-11 IEEE P802.11/D10, 14 January 1999 (hereinafter "the 802.11 standard"). The 802.11 standard specifies an Infrastructure Network that provides wireless stations access to resources on a wired local area network (LAN) by way of an access point, such as a server on the wired LAN. The Infrastructure Network can be secured using a shared key to establish a Wired Equivalency Privacy (WEP) connection between the access point and each station, such as a desktop, laptop, or handheld computer. The shared keys are distributed to the stations through secure channels outside the wireless network.

The most security is provided when the access point generates a unique shared session key for each station that may potentially connect. The session key is discarded when the connection is terminated. Because of the resources required to create and securely transmit a unique shared key to each potential station for each session, often an access point uses a single, common shared key for all stations for a given period of time, such as a day. However, each user must be informed of the common shared key for the current time period and must program it into the station. Additionally if there is a security breach so that a new common shared key is required before the time period expires, every station must be notified of the new common shared key, and each station must terminate its current session and establish a new connection.

Thus, the existing security mechanisms for wireless networks are cumbersome for the user by requiring constant manual updating of the station to reflect the current shared key, and burdensome on the access point by requiring the frequent generation of the shared keys and the distribution of those keys outside of the wireless network.

SUMMARY OF THE INVENTION

The above-mentioned shortcomings, disadvantages and problems are addressed by the present invention, which will be understood by reading and studying the following specification.

A secured wireless communications channel between an access point and a station is established by a series of message exchanged between the access point and the station. The station sends a request for a security preference for the access point to the access point. The access point sends the security preference in response to the request when the access point can support the channel. When the security preference is shared key, the station generates authentication information using a first key and sends the authentication information to the access point. The access point uses the authentication information to validate the station. If the station is valid, the access point encrypts a channel key with a second key and sends the encrypted result to the station. The station decrypts the channel key and uses it to establish the wireless channel.

The authentication information can be a user name and password, an encrypted challenge such as used in the Challenge Handshake Authentication Protocol, or other types of

data typically used to authenticate clients on a network. In one aspect, the first and second keys are identical keys. In another aspect, the first key is a public key for the access point and the second key is a public key for the station.

Using the invention, the user is required to program the station only once--when it is initially setup for the wireless network. Because each station must authenticate itself to the access point before it can establish the wireless channel using a channel key, the access point can quickly secure the network against a security breach of a common channel key by disabling the login abilities of a now-invalid user without having to terminate all the other stations or having to generate a new common channel key. Thus, the burden on the access point of generating and distributing the common channel key is greatly reduced and the security of the wireless network when using a common channel key is enhanced.

The present invention describes systems, methods, and computer-readable media of varying scope. In addition to the aspects and advantages of the present invention described in this summary, further aspects and advantages of the invention will become apparent by reference to the drawings and by reading the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram of one embodiment of a computer system environment suitable for practicing the invention;

FIG. 2 is a diagram illustrating a system-level overview of embodiments of the invention;

FIGs. 3A-B are flowcharts of a method to be performed by a station computer according to an embodiment of the invention;

FIGs. 4A-B are flowcharts of a method to be performed by an access point computer according to an embodiment of the invention; and

FIG. 5 is a diagram of an message data structure for use in an implementation of the invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following detailed description of embodiments of the invention, reference is made to the accompanying drawings in which like references indicate similar elements, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical, electrical and other changes may be made without departing from the scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims.

The following description of FIG. 1 is intended to provide an overview of computer hardware and other operating components suitable for implementing the invention, but is not intended to limit the applicable environments. Various details provided in this description are specific to Macintosh computer systems. Note, however, that the concepts of the present

invention are not limited to application to a Macintosh platform. For example, these concepts may also be applied to x86 processor based computer systems, as well as other types of computing platforms.

FIG. 1 illustrates a computer system 1 in which the present invention may be implemented. While FIG. 1 illustrates the major components of a computer system, it is not intended to represent any particular architecture or manner of interconnecting the components; such details are not germane to the present invention.

As shown, the computer system 1 of FIG. 1 includes a microprocessor 10, a read-only memory (ROM) 11, random access memory (RAM) 12, each connected to a bus system 18. The bus system 18 may include one or more buses connected to each other through various bridges, controllers and/or adapters, such as are well-known in the art. For example, the bus system may include a "system bus" that is connected through an adapter to one or more expansion buses, such as a Peripheral Component Interconnect (PCI) bus, or the like. Also coupled to the bus system 18 are a mass storage device 13, a display device 14, a keyboard 15, a pointing device 16, a communication device 17, and non-volatile RAM (NVRAM) 20. A cache memory 19 is coupled to the microprocessor 10.

Microprocessor 10 may be any device capable of executing software instructions and controlling operation of the computer system, such as a PowerPC processor, for example, or an x86 class microprocessor. ROM 11 may be a non-programmable ROM, or it may be a programmable ROM (PROM), such as electrically erasable PROM (EEPROM), Flash memory, etc.

Mass storage device 13 may include any device for storing suitably large volumes of data, such as a magnetic disk or tape, magneto-optical (MO) storage device, or any variety of Digital Versatile Disk (DVD) or compact disk ROM (CD-ROM) storage. The data is often written, by a direct memory access process, into RAM 12 during execution of software in the computer system 1. One of skill in the art will immediately recognize that the term "computer-readable medium" includes any type of storage device that is accessible by the microprocessor 10.

Display device 14 may be any device suitable for displaying alphanumeric, graphical and/or video data to a user, such as a cathode ray tube (CRT), a liquid crystal display (LCD), or the like, and associated controllers. Pointing device 16 may be any device suitable for enabling a user to position a cursor or pointer on display device 14, such as a mouse, trackball, touchpad, stylus with light pen, voice recognition hardware and/or software, etc.

Communication device 17 may be any device suitable for or enabling the computer system 1 to communicate data with a remote processing system over a communication link, such as a conventional telephone modem, a cable television modem, an Integrated Services Digital Network (ISDN) adapter, a Digital Subscriber Line (xDSL) adapter, a network interface card (NIC), an Ethernet adapter, a wireless transmitter/receiver, etc.

It will be appreciated that the computer system 1 is one example of many possible computer systems which have different architectures. The computer system of FIG. 1 may be, for example, an Apple Macintosh computer, such as an Apple iMac computer. FIG. 1 is also illustrative of personal computers based on an Intel microprocessor. Such personal computer

often have multiple buses, one of which can be considered to be a peripheral bus. Network computers are another type of computer system that can be used with the present invention. Network computers do not usually include a hard disk or other mass storage, and the executable programs are loaded from a network connection into the RAM 12 for execution by the microprocessor 10. A Web TV system, which is known in the art, is also considered to be a computer system according to the present invention, but it may lack some of the features shown in FIG. 1, such as certain input or output devices. A typical computer system will usually include at least a processor, memory, and a bus coupling the memory to the processor.

Furthermore, one of skill in the art will immediately appreciate that the invention can be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention can also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network.

It will be apparent from this description that aspects of the present invention may be embodied, at least in part, in software. That is, the technique may be carried out in a computer system in response to its microprocessor executing sequences of instructions contained in a memory, such as ROM 11, RAM 12, mass storage device 13, cache 19, or a remote storage device. In various embodiments, hardwired circuitry may be used in place of, or in combination with, software instructions to implement the present invention. Thus, the

technique is not limited to any specific combination of hardware circuitry and software, nor to any particular source for the instructions executed by a computer system.

In addition, throughout this description, various functions and operations are described as being performed by or caused by software code (or other similar phrasing) to simplify description. However, those skilled in the art will recognize that what is meant by such expressions is that the functions result from execution of the code by a processor, such as microprocessor 10.

It will also be appreciated that the computer system 1 is controlled by operating system (OS) software which includes a file management system, such as a disk operating system, which is part of the operating system software. The file management system is typically stored in the mass storage 13 and causes the microprocessor 10 to execute the various acts required by the operating system to input and output data and to store data in memory, including storing files on the mass storage 13.

A system level overview of the operation of embodiments of the invention is described with reference to FIG. 2 that illustrates the establishment 200 of a secure wireless network connection between a user station 201 and a wireless access point (AP) 203. The user station 201 and the AP 203 are computers, such as computer system 1 in FIG. 1, that are coupled together through wireless transmitter/receivers serving as communication device 17. The AP 203 is further coupled into a wired local area network (LAN) through an second communications device 17, such as a network interface card. The wireless network is secured by encrypting the data exchanged between the user station 201 and the AP 203 using a

channel key that is shared between the user station and the AP and a pre-defined shared key algorithm. The channel key can be common for all stations for a given period of time, or can be unique to each station.

The user station 201 sends a request 207 for a connection to the AP 203. If the AP 203 can handle a new connection, it sends its security preference 209, in this case "shared key," to the user station 201. The request 207 and the security preferences 209 form an inquiry sequence 205 between the station 201 and the AP 203.

In one embodiment, the station 201 and the AP 203 next perform a key exchange sequence 211 based on a pre-determined key exchange security algorithm. Station 201 chooses a secret station key and generates a value 213 using the secret station key and the key exchange security algorithm. The station 201 sends the value 213 to the AP 203. The AP 203 chooses a secret AP key and generates a self-distributed key using the secret AP key and the security algorithm. The AP 203 also generates a value 215 using the value 213, the secret AP key, and the security algorithm. The AP 203 sends the value 215 to the station 201. The station 201 uses the value 215, the secret station key, and the security algorithm to calculate the self-distributed key. It will be appreciated that the key exchange security algorithm must be mathematically constructed in a fashion that permits the station 201 to obtain the self-distributed key as described while generating values that cannot be used to determine the secret keys of either the station or the AP. One such algorithm is the Diffie-Hellman key exchange algorithm as incorporated into the Hughes transmission protocol and is as explained in more detail below.

The station 201 now authenticates itself by transmitting authentication information to the AP 203. In the present example, the station 201 encrypts the user name and password using the self-distributed key and the pre-defined shared key algorithm to create the authentication information 217 that is sent to the AP 203. The AP 203 decrypts the user name and password and checks them for validity. Assuming the user name and password are valid, the AP 203 encrypts the current channel key using the self-distributed key and the pre-defined shared key algorithm and sends the encrypted result 219 to the station 201 to complete an authentication sequence 221. Once the station 201 has decrypted the current channel key, it terminates the setup connection used by the sequences 205, 211, 221 and establishes the secure wireless network 223 by transmitting data to the AP 203 encrypted with the current channel key. In an alternate embodiment, a standard encryption algorithm, such as RC4, is substituted for the pre-defined shared key algorithm.

In another embodiment, the key exchange sequence 211 begins with the station 201 transmitting a public key 213 for the station to the AP 203. The AP 203 responds by transmitting a public key 215 for the AP to the station 201. The station 201 uses the AP public key 215 to encrypt the user name and password, and sends the authentication information 217 to the AP 203. The AP 203 decrypts the result 217 using a private key corresponding to the AP public key. After validating the user name and password, the AP 203 encrypts the current channel key with the station public key 213 and transmits the encrypted result 219 to the station 201. The station 201 decrypts the current channel key using a private

key corresponding to the station public key and terminates the setup connection prior to establishing the secure wireless network 223 as described above.

A variation on the public/private key setup connection assumes that the station 201 and the AP 203 exchange public keys using the key exchange sequence 211 only the first time a secure wireless network is established between them. Each stores the other's public key for subsequent connections. In this embodiment, the AP 203 determines which stored public key, if any, is appropriate based on a station identifier contained in the request 207. Alternatively, the public keys can be exchanged outside the wireless network.

In a further embodiment, the authentication sequence 221 uses the Challenge Handshake Authentication Protocol (CHAP). Each station is assigned a CHAP key which can be the self-distributed key created through the key exchange sequence 211 as described above, or can be an unique key chosen by either the AP 202 or the station 201 and transmitted to the other through a mechanism outside the wireless network. When the station 201 requests a connection 207, the AP 203 sends a challenge to the station 201 either as part of the security preferences 209 or as a separate message (not shown in FIG. 2). The station 201 encrypts the challenge with its CHAP key to create the authentication information 217 that is sent to the AP 203. The AP 203 also encrypts the challenge with the station's assigned CHAP key. If the authentication information 217 received from the station 201 matches the challenge as encrypted by the AP 203, the station 201 is validated and the AP 203 encrypts the current channel key with the CHAP key and sends it 219 to the station 201. In this embodiment, the

user name and password is not sent to the AP 203 across the wireless network, reducing the possibility of their being intercepted.

The authentication sequence prevents the connection of a station that is fraudulently using a common channel key and thus reduces the number of time that a common channel key must be reissued. Because the user must program the station only once, when it is initially setup for the wireless network, the invention reduces user confusion and makes the wireless network easier to use. While the invention is not limited to any particular sequence of key exchange messages, for sake of clarity a simplified sequence has been described. It will be readily apparent that other message sequences that result in the secure transmission of the authentication information and the shared channel key are equally applicable.

Next, the particular methods of the invention are described in terms of computer software with reference to a series of flowcharts shown in FIGs 3A-B and 4A-B. The methods to be performed by a computer constitute computer programs made up of computer-executable instructions. Describing the methods by reference to a flowchart enables one skilled in the art to develop such programs including such instructions to carry out the methods on suitably configured computers (the processor of the computer executing the instructions from computer-readable media). If written in a programming language conforming to a recognized standard, such instructions can be executed on a variety of hardware platforms and for interface to a variety of operating systems. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings

of the invention as described herein. Furthermore, it is common in the art to speak of software, in one form or another (e.g., program, procedure, application...), as taking an action or causing a result. Such expressions are merely a shorthand way of saying that execution of the software by a computer causes the processor of the computer to perform an action or a produce a result.

Referring first to FIG. 3A, the acts to be performed by a computer executing the station method 300 are shown. The station method 300 begins by sending a request for a connection to an AP (block 301). The request message also includes an inquiry regarding the security preferences of the AP. The response received (block 303) will indicate whether a connection is available (block 305) and if so, the type of security preference (block 307). If there is no connection available, or if the security preference is not "shared key," the security method 300 exits. It will be appreciated that an available connection using a different security preference can be established through other methods not germane to the present invention.

When necessary, a key exchange method is performed by the station computer at block 309 (shown in phantom). The key exchange method for the station corresponds to the actions described in FIG. 2 for the key exchange sequence 211. A particular embodiment using the Hughes transmission protocol for the key exchange method is described in detail below with reference to FIG. 3B. The user name and password are next encrypted using the appropriate key, e.g., the self-distributed key or the AP public key, and sent to the AP (block 311). If the AP responds with an encrypted channel key (block 313), the station can establish the secure network connection by transmitting a message encrypted with the channel key as is

conventional and not illustrated. Optionally, the method 400 terminates the initial connection before establishing the secure network connection (block 315).

The corresponding method 400 to be executed on a computer acting as the AP is illustrated in FIG. 4A. The AP method 400 receives the request from the station at block 401, determines if there is an available connection (block 403) and responds with the AP security preferences if so (block 405). The AP computer next performs a key exchange method at block 407 when required. A embodiment for the AP key exchange method using the Hughes transmission protocol is described in detail below with reference to FIG. 4B.

When the AP computer receives the encrypted user name and password (block 411), the method 400 decrypts and validates the user name and password against the valid users for the AP (block 411). Assuming the user name and password are valid (block 413), the AP method encrypts the current channel key for the station using the appropriate key, e.g., the station public key or the self-distributed key, and sends the encrypted result to the station (block 413). The participation of the AP in the subsequently-established secure network is well-known and not illustrated. The embodiment illustrated in FIG. 4A returns error messages to the station at block 417 when a connection is not available or when the user name and password cannot be validated.

Turning now to FIGs. 3B and 4B, one embodiment of key exchange methods 320, 420 for the station and AP is described. The key exchange is based on the Hughes transmission protocol which incorporates the Diffie-Hellman security algorithm shown in formula 1 in which n, g and p are large integers, such that g is less than p but greater than 1.

(formula 1) $k = g^n \bmod p$

The AP chooses a value for n for each station and generates a unique shared secret key k using formula 1. The values of n assigned to the stations are kept secret by the AP However, because it is difficult to calculate n given the result of the security algorithm, the values of g and p do not have to be secret, nor do they have to be unique to each station. In one embodiment, the values of g and p are sent to the station by the AP as part of the response message at block 307 in FIG. 3A. In an alternate embodiment, the values of g and p are given to a user when the user's name and password are initially registered with the AP. The user then inputs the values to the station. In still another embodiment, the AP publishes the values of g and p and all stations use the same values. One advantage of using the same values of g and p for all stations, is that the values can be hardcoded into the stations, and all APs, when they are manufactured, eliminating the complexity of distributing the values through the network and also eliminating errors inherent in having the user manually input the values to a station.

In the interest of clarity, the acts performed by the computers executing the station and the AP key exchange methods 320, 420 are described in an interleaved fashion, beginning with the key exchange method for the AP 420.

As described above, the AP selects a random large integer x to be the unique value of n for the station (the secret AP key) and generates the self-distributed key k using formula 1 (block 421 in FIG. 4B). Similarly, the station selects a random large integer y (the secret station key) and calculates a value Y using formula 2 (block 321 in FIG. 3B).

(formula 2) $Y = g^y \bmod p$

The station sends Y to the AP (block 323). When the AP receives Y, it generates a value X using formula 3 (block 423), which it sends to the station (block 425).

(formula 3) $X = Y^x \bmod p$

The station calculates k from X using formulas 4 and 5 (block 325).

(formula 4) $z = y^{-1}$

(formula 5) $k = X^z \bmod p$

At this point, both the station and the AP are in possession of the self-distributed key k and can begin the encrypted authentication process described previously. One of the advantages of the Hughes transmission protocol is that it places the majority of the calculation burden on the station, not the AP, thus allowing the AP to service more stations simultaneously.

The particular methods performed by a station and AP for an embodiment of the invention have been described. The method performed by a computer acting as a station has been shown by reference to a flowchart in FIG. 3A including all the acts from 301 until 315. The method performed by a computer acting as an access point by reference to a flowchart in FIG. 4A including all the acts from 401 until 417. Additionally, the use of the Hughes key exchange protocol in an embodiment of the invention has been shown by reference to flowcharts in FIGs. 3B and 4B including all the acts from 321 until 325 and from 421 until 425, respectively.

The invention is particularly suited for use with Infrastructure Networks defined by the 802.11 standard. An Infrastructure Network provides wireless stations access to resources on a wired LAN by way of an AP. The AP specifies whether access to the LAN is open to all stations ("Open System") or secured through a Wired Equivalent Privacy (WEP) protocol using a shared key and a WEP encryption algorithm ("Shared Key"). The 802.11 standard assumes that the shared WEP key is distributed though some secure channel prior to creating the WEP connection between the AP and a station. The invention provides such a secure channel as described above by exchanging messages between the station and the AP using the 802.11 standard message format. In one embodiment shown in FIG. 5, a data structure 500 for the invention's messages corresponds to an 802.11 management frame for authentication information. It will be appreciated that only the fields germane to the invention are illustrated in FIG. 5 and that one of skill in the art will readily understand the location and use of the omitted fields upon reading the following description in light of the 802.11 standard.

Fields 501 and 503 contains values that define the type and sub-type of the data structure, respectively, i.e., management and authentication. A station address field 505 contains a value for the station identity for those messages sent from the station to the AP. Fields 507, 509, 511, and 513 collectively form a frame body 515 for the message and contain information specific to the message being transmitted as described next.

The particular messages used by the invention can be divided into two groups. The first group is referred to as the AP's Choice group and contains the messages 207, 209 of the inquiry sequence 205 in FIG. 2. The second group is referred to as the Name and Password

group and contains the messages 213, 215 for the key exchange sequence 211 and the messages 217, 219 for the authentication sequence 221. The message data structures are described next with reference to the corresponding messages in FIG. 2.

The frame body 515 for an inquiry message 207 from the station to the AP specifies that is it a request for AP's Choice of authentication algorithm in the authentication algorithm identifier field 507 and the number "1" in the authentication transaction sequence number field 509. The other fields are empty. The AP responds with a security preferences message 209 containing a value for its preferred method of authentication in field 507, e.g. Shared Key or Open System, and a sequence number of "2" in field 509 if a connection is available. If a connection is unavailable, the message 209 contains an error code in the status code field 511.

Assuming that a connection is available and that the AP's choice of authentication is Shared Key, in an embodiment using the Hughes key exchange protocol, the station sends a message 213 containing a value for name and password authentication in field 507 and the value of *Y* (calculated by the station using the Diffie-Hellman algorithm as described above) in the authentication algorithm dependent information field 513. The sequence number in field 509 is "1." The AP responds with a message 215 containing the same value in field 507, the value of *X* in field 513, and a sequence number of "2" in field 509.

The key exchange sequence 211 is now complete because the station has the information necessary to calculate the self-distributed key as described previously. The station begins the authentication sequence 221 by using the WEP encryption algorithm to encrypt the user name and password with the self-distributed key and storing the result in field

513 of the message 217 and a sequence number of "3" in field 509. Field 507 contains the name and password authentication value as before. The AP decrypts the user name and password and validates them. If the user name or password are valid, the AP encrypts the shared WEP key, i.e. the shared channel key, with the self-distributed key and stores the result in field 513 to create message 219. The AP also stores the value associated with Shared Key authentication in field 507, and a "4" in field 509. If the user name or password are invalid, the message 219 contains an error code in the status code field 511 and no data in field 513.

The establishment of a secured wireless network channel between a station and an access point has been described that requires the user to program his or her station only once while simultaneously enhancing the security of a wireless network that uses a common shared key. A particular embodiment has also been described that uses the Hughes transmission protocol to reduce the processing burden on the AP, thus enabling the AP to service more stations simultaneously. An embodiment applicable for use with an IEEE 802.11 Infrastructure Network uses a message data structure that conforms to the format specified by the 802.11 standard, allowing use of the invention in such networks while adhering to the standard.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the present invention.

The terminology used in this application with respect to networks, both wired and wireless, is meant to include all such network environments. Therefore, it is manifestly intended that this invention be limited only by the following claims and equivalents thereof.

CLAIMS

What is claimed is:

1. A method of establishing a secure wireless communications channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

sending, by the station to the access point, a request for a security preference for the access point;

sending, by the access point to the station, the security preference in response to the request when the access point can support the channel;

generating, by the station, authentication information using a first key when the security preference is shared key;

sending, by the station to the access point, the authentication information;

validating, by the access point, the station using the authentication information;

encrypting, by the access point, the channel key using a second key when the station is validated;

sending, by the access point to the station, the encrypted channel key;

decrypting, by the station, the channel key in response to receiving the encrypted channel key; and

sending, by the station to the access point, data encrypted with the channel key to establish the channel.

2. The method of claim 1, wherein the first and second keys are a self-distributed key.

3. The method of claim 2, further comprising:

generating, by the access point, the self-distributed key using a security algorithm when the security preference is shared key;

generating, by the station and sending to the access point, a first value using the security algorithm in response to receiving the security preference of shared key;

generating, by the access point, and sending to the station, a second value using the security algorithm and the first value in response to receiving the first value; and

calculating, by the station, the self-distributed key using the security algorithm and the second value in response to receiving the second value.

4. The method of claim 3, wherein the security algorithm is $g^n \bmod p$ and further comprising:

obtaining, by the access point, integers x, g and p to generate the self-distributed key $k = g^x \bmod p$;

obtaining, by the station, the integers g and p, and an integer y to generate the first value $Y = g^y \bmod p$;

generating, by the access point, the second value $X = Y^x \bmod p$; and

setting, by the station, z equal to y^{-1} to calculate the self-distributed key $k = X^z \bmod p$.

5. The method of claim 4 wherein obtaining, by the station, the integers g and p comprises:

sending, by the access point to the station, the integers for g and p.

6. The method of claim 5, wherein the integers for g and p are sent to the station when the security preferences are sent by the access point.

7. The method of claim 5, wherein the integers for g and p are sent to the station when a user name and password for the station are registered with the access point.

8. The method of claim 4 further comprising:

publishing, by the access point, the integers g and p for a set of stations.

9. The method of claim 2 further comprising:

encrypting, by the station, a name and password with the first key to generate the authentication information; and

decrypting, by the access point, the name and password to validate the station.

10. The method of claim 2 further comprising:

sending, by the access point to the station, a challenge;

encrypting, by the station, the challenge with the first key to generate the authentication information;

encrypting, by the access point, the challenge with the first key; and

comparing, by the access point, the authentication information with the challenge encrypted by the access point with the first key to validate the station.

11. The method of claim 1, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

12. The method of claim 11 further comprising:

sending, by the access point to the station, the first key; and.

sending, by the station to the access point, the second key.

13. The method of claim 12, wherein the second key is sent to the access point when the request for the security preference is sent by the station.

14. The method of claim 12, wherein the first key is sent to the station when the security preference is sent by the access point.

15. The method of claim 1, wherein establishing the channel creates a standard wired equivalent privacy (WEP) network, and the station and the access point exchange messages conforming to a format required by the standard that defines a WEP network to establish the WEP network.

16. A method for connecting a station to a secure wireless network comprising:

sending a request for a security preference to an access point for the secure wireless network;

generating authentication information for the station when the station receives a security preference specifying shared key from the access point;

sending the authentication information to the access point;

decrypting a channel key in response to receiving an encrypted channel key from the access point; and

sending data encrypted with the channel key to the access point.

17. The method of claim 16 further comprising:

generating a first value using a security algorithm in response to receiving the security preference specifying shared key from the access point;

calculating a self-distributed key using the security algorithm and a second value in response to receiving the second value from the access point; and

using the self-distributed key to generate the authentication information and to decrypt the encrypted channel key.

18. The method of claim 17, wherein the security algorithm is formulated as $g^n \bmod p$ and further comprising:

obtaining integers for y, g and p to generate the first value $Y = g^y \bmod p$; and

setting z equal to y^{-1} to calculate the self-distributed key $k = X^z \bmod p$.

19. The method of claim 16 further comprising:

using a first key to generate the authentication information; and

using a second key to decrypt the encrypted channel key.

20. The method of claim 19, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a private key of a public-private key pair for the station.

21. A method of securing a wireless network at an access point comprising:

sending a security preference in response to a request from a station;

validating the station in response to receiving authentication information from the station;

encrypting a channel key when the station is validated;

sending the encrypted channel key to the station; and

sending data encrypted with the channel key to the station.

22. The method of claim 21 further comprising:

generating a self-distributed key using a security algorithm when the security preference is shared key;

generating a second value using the security algorithm and a first value in response to receiving the first value from the station; and

sending the second value to the station.

23. The method of claim 22, wherein the security algorithm is formulated as $g^n \bmod p$ and further comprising:

obtaining integers x, g and p to generate the self-distributed key $k = g^x \bmod p$; and

generating the second value $X = Y^x \bmod p$.

24. The method of claim 21 further comprising:

using a first key to evaluate the authentication information; and

using a second key to encrypt the encrypted channel key.

25. The method of claim 24, wherein the first key is a private key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

26. A computer-readable medium having stored thereon executable instructions to cause a processor to perform a station method to connect to a secure wireless network, the instructions comprising:

sending a request for a security preference to an access point for the secure wireless network;

generating authentication information for the station when the station receives a security preference specifying shared key from the access point;

sending the authentication information to the access point;

decrypting a channel key in response to receiving an encrypted channel key from the access point; and

sending data encrypted with the channel key to the access point.

27. The computer-readable medium of claim 26 having further instructions comprising:

generating a first value using a security algorithm in response to receiving the security preference specifying shared key from the access point;

calculating a self-distributed key using the security algorithm and a second value in response to receiving the second value from the access point; and

using the self-distributed key to generate the authentication information and to decrypt the encrypted channel key.

28. The computer-readable medium of claim 27, wherein the security algorithm is formulated as $g^n \ mod \ p$ and having further instructions comprising:

obtaining integers y, g and p to generate the first value $Y = g^y \ mod \ p$; and

setting z equal to y^{-1} to calculate the self-distributed key $k = X^z \ mod \ p$.

29. The computer-readable medium of claim 26 having further instructions comprising:

using a first key to generate the authentication information; and

using a second key to decrypt the encrypted channel key.

30. The computer-readable medium of claim 29, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a private key of a public-private key pair for the station.

31. A computer-readable medium having stored thereon executable instruction to cause a processor to perform an access point method to secure a wireless network, the instructions comprising:

sending a security preference in response to a request from a station;

validating the station in response to receiving authentication information from the station;

encrypting a channel key when the station is validated;

sending the encrypted channel key to the station; and

sending data encrypted with the channel key to the station.

32. The computer-readable medium of claim 31 having further instructions comprising:

generating a self-distributed key using a security algorithm when the security preference is shared key;

generating a second value using the security algorithm and a first value in response to receiving the first value from the station; and

sending the second value to the station.

33. The computer-readable medium of claim 32, wherein the security algorithm is formulated as $g^n \bmod p$ and having further instructions comprising:

obtaining integers x, g and p to generate the self-distributed key $k = g^x \bmod p$; and

generating the second value $X = Y^x \bmod p$.

34. The computer-readable medium of claim 31 having further instructions comprising:

using a first key to evaluate the authentication information; and

using a second key to encrypt the encrypted channel key.

35. The computer-readable medium of claim 34, wherein the first key is a private key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

36. A secure wireless network comprising:

an access point operable for receiving a connection request from a station through a setup connection, for validating authentication information sent by the station, and for connecting the station to the network through a channel secured with a shared channel key; and

a station operable for sending the connection request to the access point, and for generating the authentication information to send to the access point.

37. The secure wireless network of claim 36, wherein the access point is further operable for sending a security preference specifying shared key to the station upon receiving the connection request, and the station is operable for sending the authentication information to the station upon receiving a security preference specifying shared key.

38. The secure wireless network of claim 37, wherein the access point is further operable for encrypting the shared channel key using a self-distributed key for sending to the station and the station is further operable for decrypting the shared channel key upon receipt.

39. The secure wireless network of claim 38, wherein the station and the access point are further operable for calculating the self-distributed key by exchanging messages in accordance with the Hughes transmission protocol

40. The secure wireless network of claim 36, wherein the station is further operable for using a first key to generate the authentication information and for using a second key to decrypt an encrypted shared channel key received from the access point, and the access point is further operable for using a third key to evaluate the authentication information and for using a fourth key to encrypt the shared channel key for sending to the station.

41. The secure wireless network of claim 40, wherein the first and third keys are public and private keys, respectively, for the access point, and the second and fourth keys are private and public keys, respectively, for the station.

42. A computer-readable medium having stored thereon a message data structure for a secure wireless network comprising:

a station address field containing data representing an identifier for a station that exchanges messages with an access point on the secure wireless network;

a transaction sequence number field containing data representing a sequence number for a message exchanged between the station identified by the station address field and the access point;

an authentication algorithm field containing data representing an identifier for a protocol used by the access point to validate the station identified by the station address field based on a name and password for the station; and

a dependent information field containing data required to connect the station identified by the station address field to the secure wireless network.

43. The computer-readable medium of claim 42, wherein the data in the dependent information field represents key information for encrypting the name and password for the station identified by the station address field.

44. The computer-readable medium of claim 42, wherein the data in the dependent information field represents an encrypted name and password for the station identified by the station address field.

45. The computer-readable medium of claim 42, wherein the data in the dependent information field represents an encrypted channel key used to connect the station identified by the station address field to the secure wireless network.

ABSTRACT OF THE DISCLOSURE

A wireless network is established between a station and an access point for the network using a sequence of messages that securely transmit authentication information from the station to the access point for validation by the access point, and subsequently transmit a shared key necessary to establish the wireless network from the access point to the station when the station is validated.

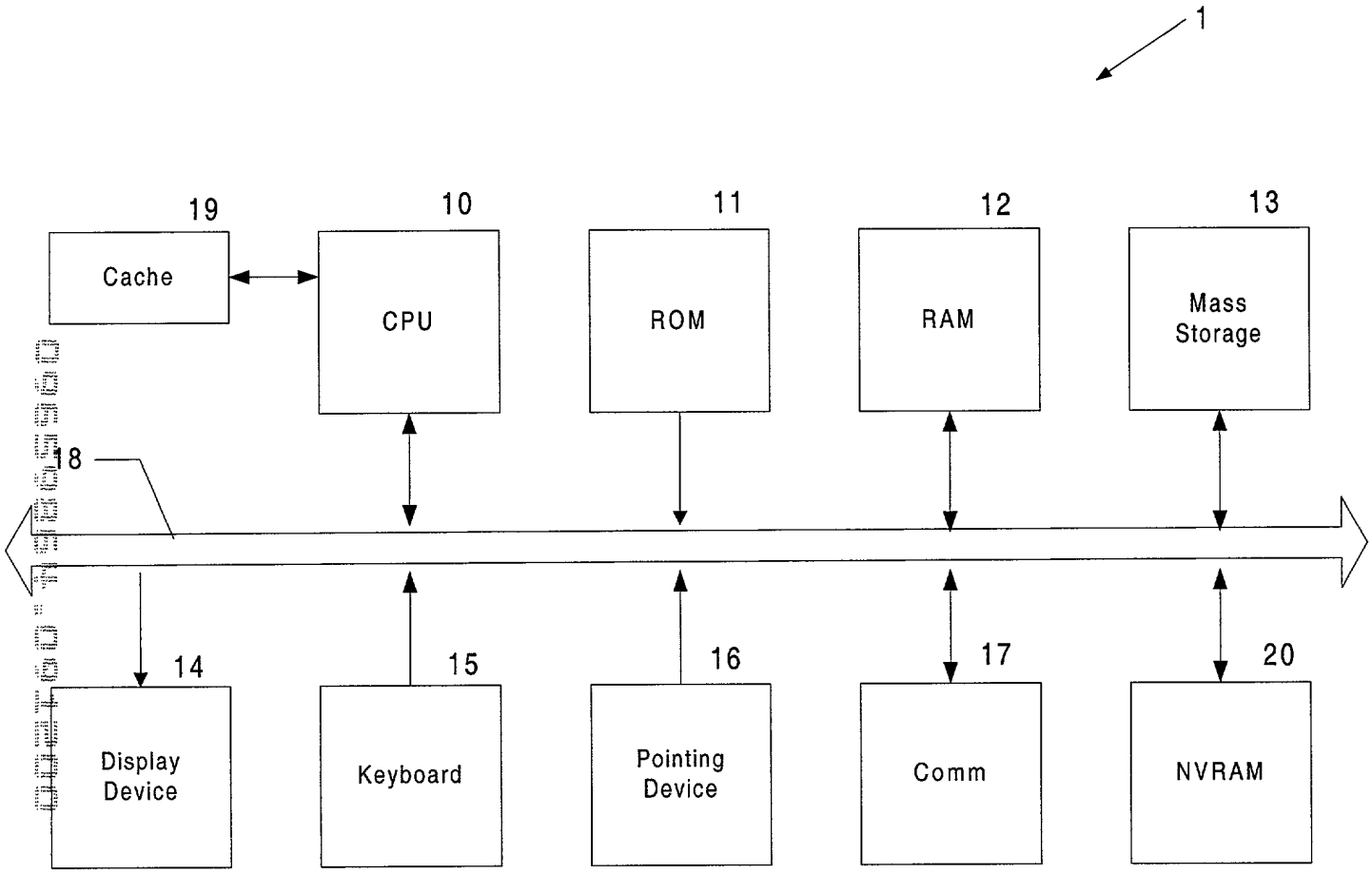
1
19
Cache
10
CPU
11
ROM
12
RAM
13
Mass Storage
18
14
Display Device
15
Keyboard
16
Pointing Device
17
Comm
20
NVRAM

FIG. 1

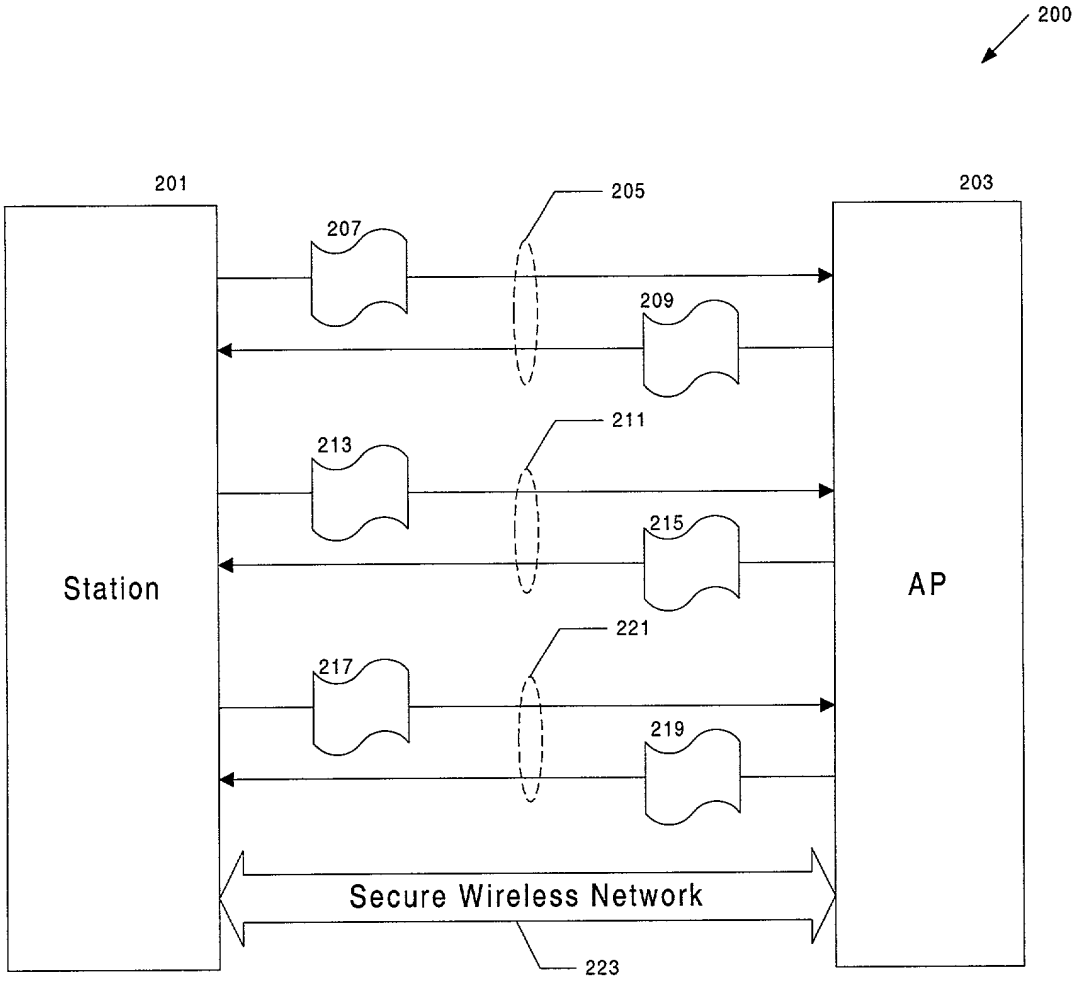
200
201
203
205
207
209
211
213
215
217
219
221
Station
AP
Secure Wireless Network
223

FIG. 2

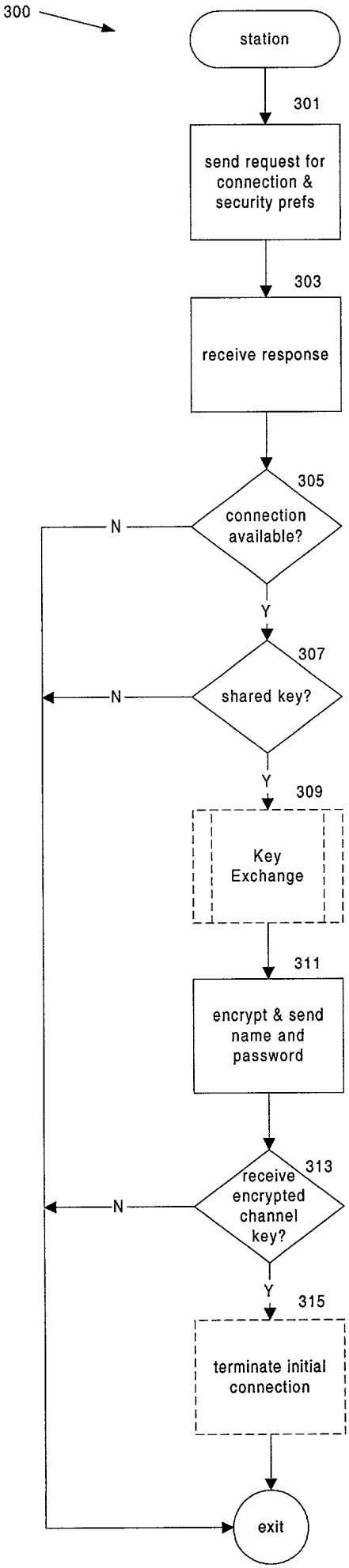
300
station
301
send request for connection & security prefs
303
receive response
305
connection available?
N
Y
307
shared key?
N
Y
309
Key Exchange
311
encrypt & send name and password
313
receive encrypted channel key?
N
Y
315
terminate initial connection
exit

FIG. 3A

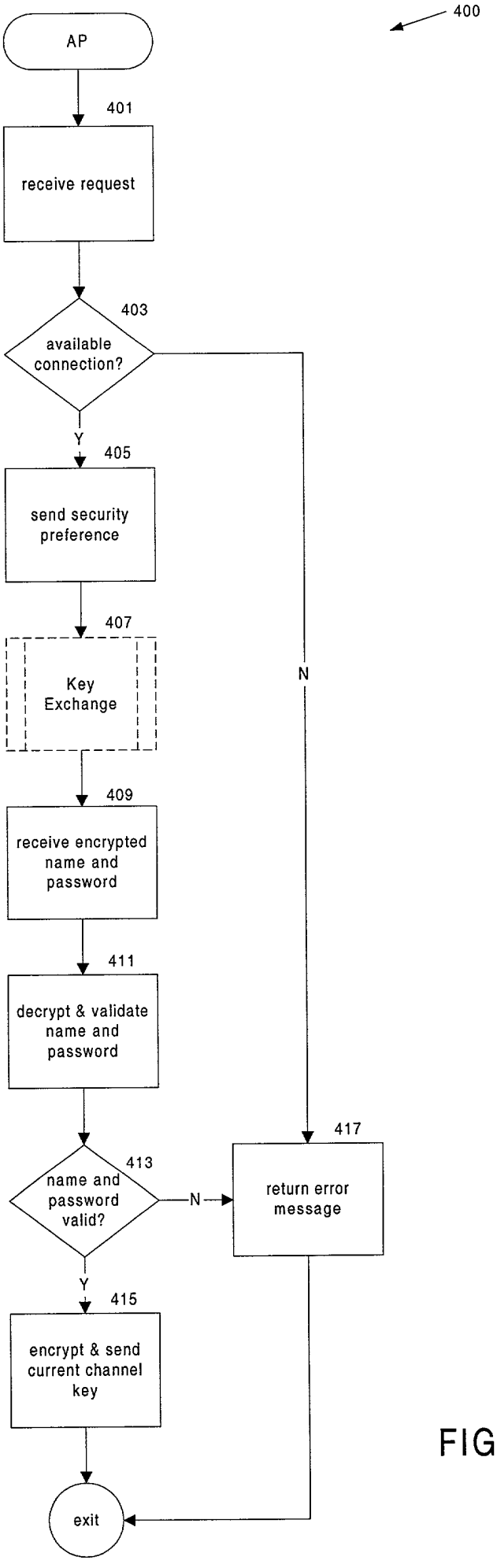
400
AP
401
receive request
403
available connection?
Y
N
405
send security preference
407
Key Exchange
409
receive encrypted name and password
411
decrypt & validate name and password
413
name and password valid?
N
Y
415
encrypt & send current channel key
417
return error message
exit

FIG. 4A

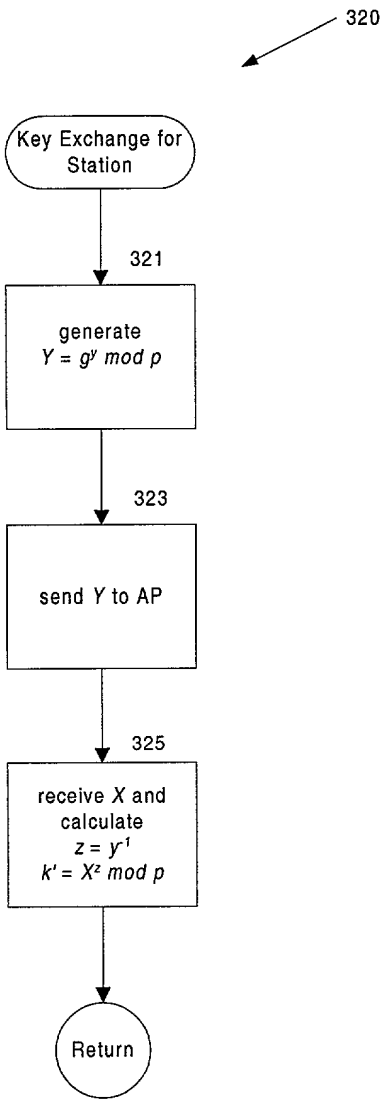
320
Key Exchange for Station
321
generate
$Y = g^y \bmod p$
323
send Y to AP
325
receive X and calculate
$z = y^{-1}$
$k' = X^z \bmod p$
Return

FIG. 3B

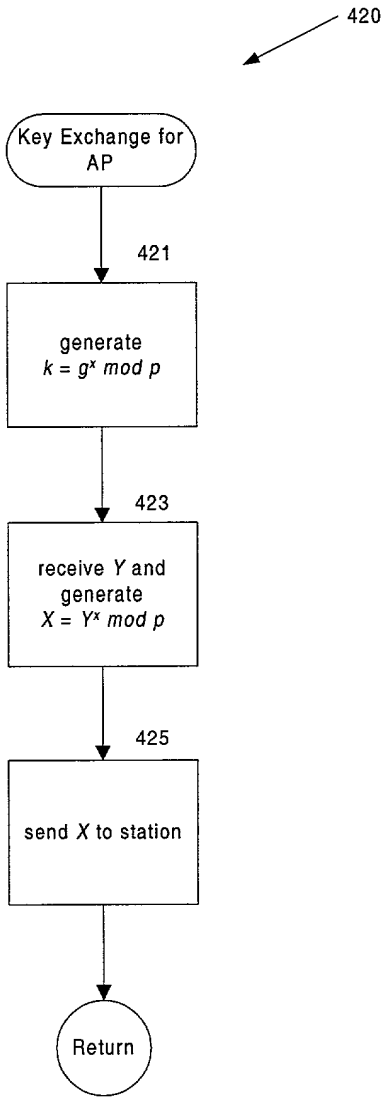
420
Key Exchange for AP
421
generate
$k = g^x \bmod p$
423
receive Y and generate
$X = Y^x \bmod p$
425
send X to station
Return

FIG. 4B

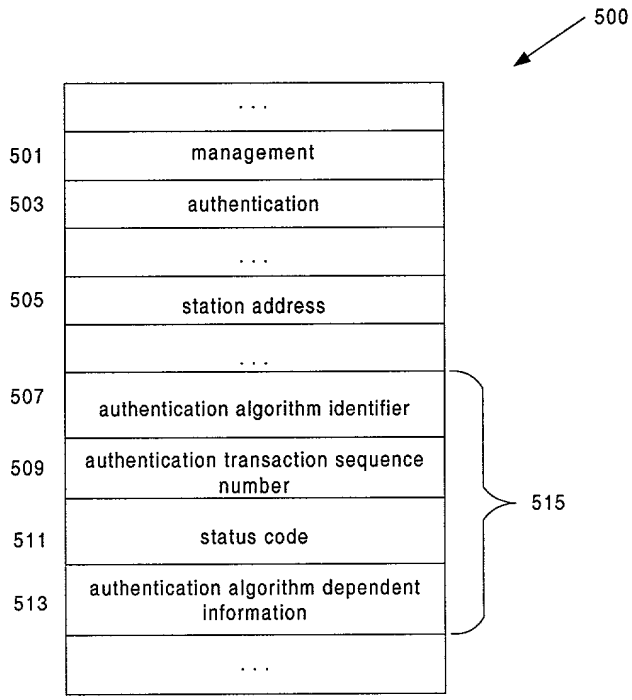
500
. . .
501
management
503
authentication
. . .
505
station address
. . .
507
authentication algorithm identifier
509
authentication transaction sequence number
511
status code
513
authentication algorithm dependent information
515
. . .

FIG. 5

Attorney's Docket No.: 004860.P2436 Patent

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

USER CONTROL OF A SECURE WIRELESS COMPUTER NETWORK

the specification of which

x is attached hereto.

___ was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____ .
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority Claimed

(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

(Application Number)	Filing Date
(Application Number)	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Number)	Filing Date	(Status -- patented, pending, abandoned)
(Application Number)	Filing Date	(Status -- patented, pending, abandoned)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to **Sheryl Sue Holloway** (Name of Attorney or Agent), BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to **Sheryl Sue Holloway** (Name of Attorney or Agent), (408) 720-8598.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor "J" Leslie Vogel III

Inventor's Signature _____ Date 4/2/00

Residence Sausalito, California (City, State) Citizenship United States (Country)

Post Office Address 26 Gate 6½ Rd.
Sausalito, California 94965

<u>APPENDIX A</u>

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, under 37 C.F.R. § 10.9(b); Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Sanjeet Dutta, Reg. No. P46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Eric T. King, Reg. No. 44,188; Kurt P. Leyendecker, Reg. No. 42,799; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Marina Portnova, Reg. No. 45,750; Babak Redjaian, Reg. No. 42,096; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. P46,322; Thomas C. Webster, Reg. No. P46,154; Charles T. J. Weigell, Reg. No. 43,398; Kirk D. Williams, Reg. No. 42,229; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Justin M. Dillon, Reg. No. 42,486; my patent agent, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and James R. Thein, Reg. No. 31,710, my patent attorney. I also hereby appoint Albert P. Cefalo, Reg. No. 27,315; Mark Aaker, Reg. No. 32,667, Richard Liu, Reg. No. 34,377; Helene Plotka Workman, Reg. No. 35,981; and Edward W. Scott, IV, Reg. No. 36,000; my attorneys; of APPLE COMPUTER, INC., located at 1 Infinite Loop, MS: 3-PAT, Cupertino, California 95014, telephone (408)974-9453, will full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

APPENDIX B

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.